IN THE SPECIFICATION

Please amend the paragraph at page 4, lines 1-7, as follows:

Referring to Fig. 1, reference numeral 1 shows an identification system according to this embodiment, in which a plurality of encryption devices 2 (2A to 2N) serving as communication sources are wirelessly connected to a decryption device 3 serving as a communication party so that the encryption devices 2 and the decryption device 3 can ~~communication~~ communicate various kinds of information with each other.

Please amend the paragraph beginning at page 4, line 25 to page 5, line 2, as follows:

As described above, in this identification system 1, ~~validly~~ validity of a user using the encryption device 2 is determined by using body information on the user.

Please amend the paragraph at page 6, lines 5-11, as follows:

In addition, the imaging unit 11 is provided with a diffusion plate [[25]] 26 at a position (hereinafter, referred to as out-of-light-path position) P1 other than on the light path of the near-infrared light. This diffusion plate [[25]] 26 can move between the out-of-light-path position P1 and a position (hereinafter, referred to as on-light-path position) P2 a prescribed distance away from the solid imaging element 24.

Please amend the paragraph at page 6, lines 12-19, as follows:

Furthermore, in this imaging unit 11, a finger FG can be inserted between the first filter 22 and the second filter 23, and a shielding unit [[26]] 25 for blocking the outside light in the air out of the light path of the near-infrared light while the finger FG is inserted is provided, thereby being capable of reducing influences of visible light and ultraviolet radiation existing out of the shielding unit [[26]] 25 on the near-infrared light in imaging the blood vessels inside the finger FG.

Please amend the paragraph at page 9, lines 14-18, as follows:

In actual, the encryption key information creation unit 15 controls the diffusion plate [[25]] 26 of the imaging unit 11 (Fig. 3) so as to move from the out-of-light-path position P1 to the on-light-path position P2, and sends an imaging command to the imaging unit 11.

Please amend the paragraph at page 9, lines 19-25, as follows:

In this case, in the imaging unit 11 (Fig. 3), the diffusion plate [[25]] 26 is irradiated with near-infrared light emitted from the light sources 21 via the first and second filters 22 and 23 in order, and diffuses the light toward the solid imaging element 24 as uniform diffused light (hereinafter, referred to as uniform diffused light), so that the light enters the solid imaging element 24.

Please amend the paragraph at page 10, lines 20-24, as follows:

In this embodiment, as a method of creating the element-specific parameter, the encryption key information creation unit 15 calculates a ~~humming~~ hamming distance of a uniform image data and a prescribed evaluation pattern data and creates an element-specific parameter from the calculation result.

Please amend the paragraph beginning at page 10, line 25 to page 11, line 19, as follows:

Specifically, the encryption key information creation unit 15 has an information memory 15a storing, for example, three data strings which are different in ~~humming~~

hamming distance, as evaluation patterns A_{EV}, B_{EV}, and C_{EV}. By using these evaluation patterns A_{EV}, B_{EV}, and C_{EV}, taking as "X" higher-ranked uniform image data (hereinafter, referred to as higher-ranked uniform image data) of the same data length as the evaluation patterns out of the uniform image data, and taking an eXclusive OR (XOR) as "^", and with the following equation,

$$\begin{aligned} dH(x, A_{EV}) &= \sum xi\text{\textasciicircum}Ai = Xa \\ dH(x, B_{EV}) &= \sum xi\text{\textasciicircum}Bi = Xb \qquad \text{.....(1)} \\ dH(x, C_{EV}) &= \sum xi\text{\textasciicircum}Ci = Xc \\ &\text{where } i = 1 \text{ to } n \end{aligned}$$

the encryption key information creation unit 15 calculates the ~~humming~~ hamming distance Xa, Xb, Xc of the higher-ranked uniform image data Z and each of the evaluation patterns A_{EV}, B_{EV}, and C_{EV}, and combines the ~~humming~~ hamming distances Xa, Xb and Xc, thereby creating an element-specific parameter.

Please amend the paragraph at page 13, lines 16-24, as follows:

The decryption device 3 is composed of a communication unit 30 for communicating information through a communication process under a prescribed radio communication scheme, a requesting unit 31 for making various requests to the encryption devices 2 (2A to 2N), a ~~decryption~~ decoding unit 32 for decrypting encrypted identification information D3 received via the communication unit 30, a comparison unit 33 for performing a prescribed identification process by using a decryption result of the ~~decryption~~ decoding unit 32, and a registration database DB.

Please amend the paragraph at page 14, lines 7-14 as follows:

In this case, the requesting unit 31 requests an encryption device 2 (2A to 2N) being connected via the communication unit 30, for various conditions for an identification process at prescribed timing. The conditions include the number of encryption key information $D2_1$, $D2_2$,..., $D2_n$ to be used out of a plurality of encryption key information, and other matters. In this case, the ~~decryption~~ decoding unit 32 is notified of the number of specified encryption key information.

Please amend the paragraph beginning at page 14, line 23 to page 15, line 5, as follows:

The ~~decryption~~ decoding unit 32 reads registration information $D10_1$ corresponding to, for example, the encryption device 2A from the registration database DB based on a transmission source address written in the header of encryption identification information D3 supplied via the communication unit 30, and selects encryption information $D2_1$ notified from the requesting unit 31 out of the plurality of encryption key information $D2_1$ to $D2_n$ of the registration information $D10_1$.

Please amend the paragraph at page 15, lines 6-11 as follows:

The ~~decryption~~ decoding unit 32 restores the identification information D1 by performing the same encryption process as the encryption device 2A, on the encrypted identification information D3 by using the encryption key information $D2_1$ being selected, and sends the identification information D1 and corresponding registration information $D10_1$ to the comparison unit 33.

Please amend the paragraph at page 16, lines 16-22, as follows:

Therefore, the encryption device 2 (2A to 2N) is capable of creating encryption key information D2 obtained from the element-specific parameter, which can not be known by third parties even in manufacturing, without previously storing encryption keys in a non-volatile memory, unlike conventional systems, resulting in being capable of ensuring confidentiality of the identification information D1 easily.

Please amend the paragraph beginning at page 17, line 23 to page 18, line 16, as follows:

Further, the above embodiment has described a case where the creation means creates a unique parameter by directly calculating ~~humming~~ hamming distances (correlation values) between data of the uniform image signal S2 output from an element group and three different evaluation patterns A_{EV}, B_{EV}, and C_{EV} being stored in an information memory serving as a storage means and combining the calculation results in a prescribed order. This invention, however, is not limited to this and FFT (Fast Fourier Transform) can be performed on data of the uniform image signal S2 and calculation results of ~~humming~~ hamming distances of this result and the evaluation patterns A_{EV}, B_{EV}, and C_{EV} can be combined. Alternatively, an inverse FFT can be performed on only data of low frequency components out of a result of the FFT, and the results of ~~humming~~ hamming distances of the FFT result and the evaluation patterns A_{EV}, B_{EV}, and C_{EV} can be combined. Or these processing results can be combined. By doing this, a unique parameter with high confidentiality and repeatability can be created, thus making is possible to significantly improve reliability of the encryption function.

Please amend the paragraph at page 18, lines 17-25, as follows:

In this case, the encryption key information creation unit 15 makes the imaging unit 11 image the diffusion plate [[25]] 26 and creates a unique parameter as encryption key information based on a signal obtained as the imaging result. This invention, however, is not limited to this and the imaging unit 11 can image another uniform imaging target other than the diffusion plate [[25]] 26, or only a unique parameter can be created without creating the encryption key information. In short, another kind of creation unit for creating a unique parameter can be used.